



HAL
open science

Towards Low-Power and Low Data-Rate Software-Defined Radio Baseband with RISC-V Processor for Flexibility and Security

Mohamed El-Bouazzati, Philippe Tanguy, Guy Gogniat

► **To cite this version:**

Mohamed El-Bouazzati, Philippe Tanguy, Guy Gogniat. Towards Low-Power and Low Data-Rate Software-Defined Radio Baseband with RISC-V Processor for Flexibility and Security. 15ème Colloque National du GDR SOC2, Jun 2021, Rennes, France. hal-04164388

HAL Id: hal-04164388

<https://hal.science/hal-04164388>

Submitted on 18 Jul 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Towards Low-Power and Low Data-Rate Software-Defined Radio Baseband with RISC-V Processor for Flexibility and Security



Mohamed EL-BOUZZATI, Philippe TANGUY, Guy GOGNIAT
 Lab-STICC, team ARCAD, Université Bretagne Sud
 firstname.lastname@univ-ubs.fr

Abstract

This work discusses opportunities and challenges of using Software Defined Radio (SDR) in baseband processor architectures dedicated to IoT end-devices.

It highlights some important features that are still missing to build flexible, secure and low-power SDR processors for IoT end-devices using Sub-GHz low data rate protocols.

SDR baseband architectures related work

This table presents a comparison of IoT SDR baseband processor architectures and their features:

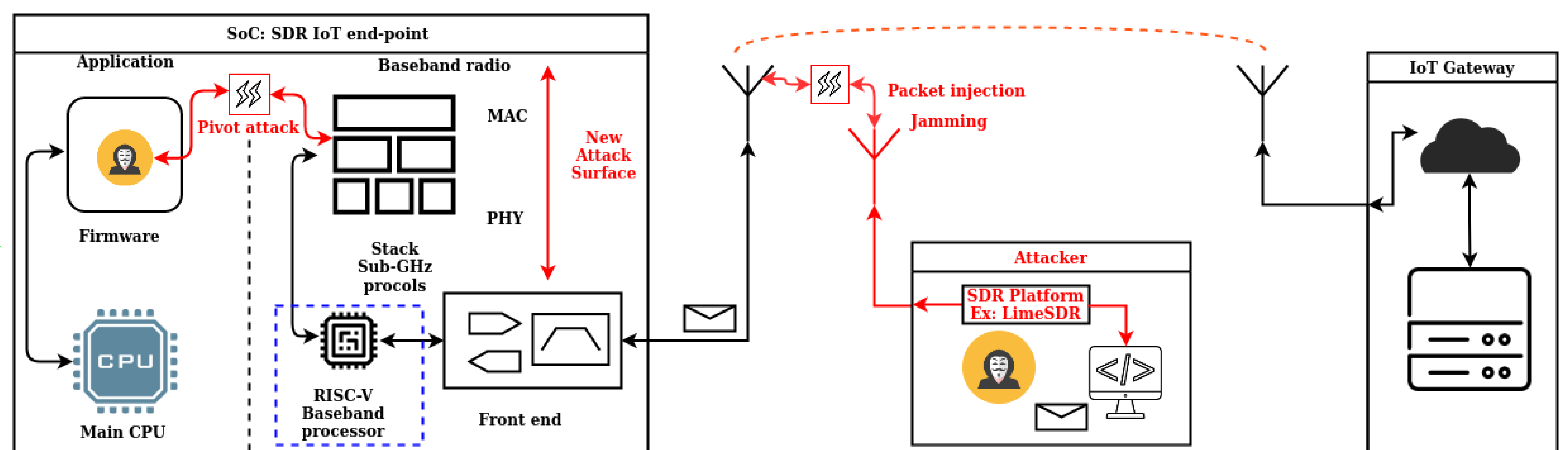
Architecture	Hybrid FPGA [1]	CPU (dedicated) [2]	CPU (Generic) [3]	ARM cortex M0+
Multi-Protocol operation	X	X	X	X
Programmability	+	+	+++	+++
Security	X	X	X	✓
Flexibility	+++	+	++	++
Dynamic power	~ 100mW	~ 10mW	~ 10μW	~ 10μW

State of the art regarding security

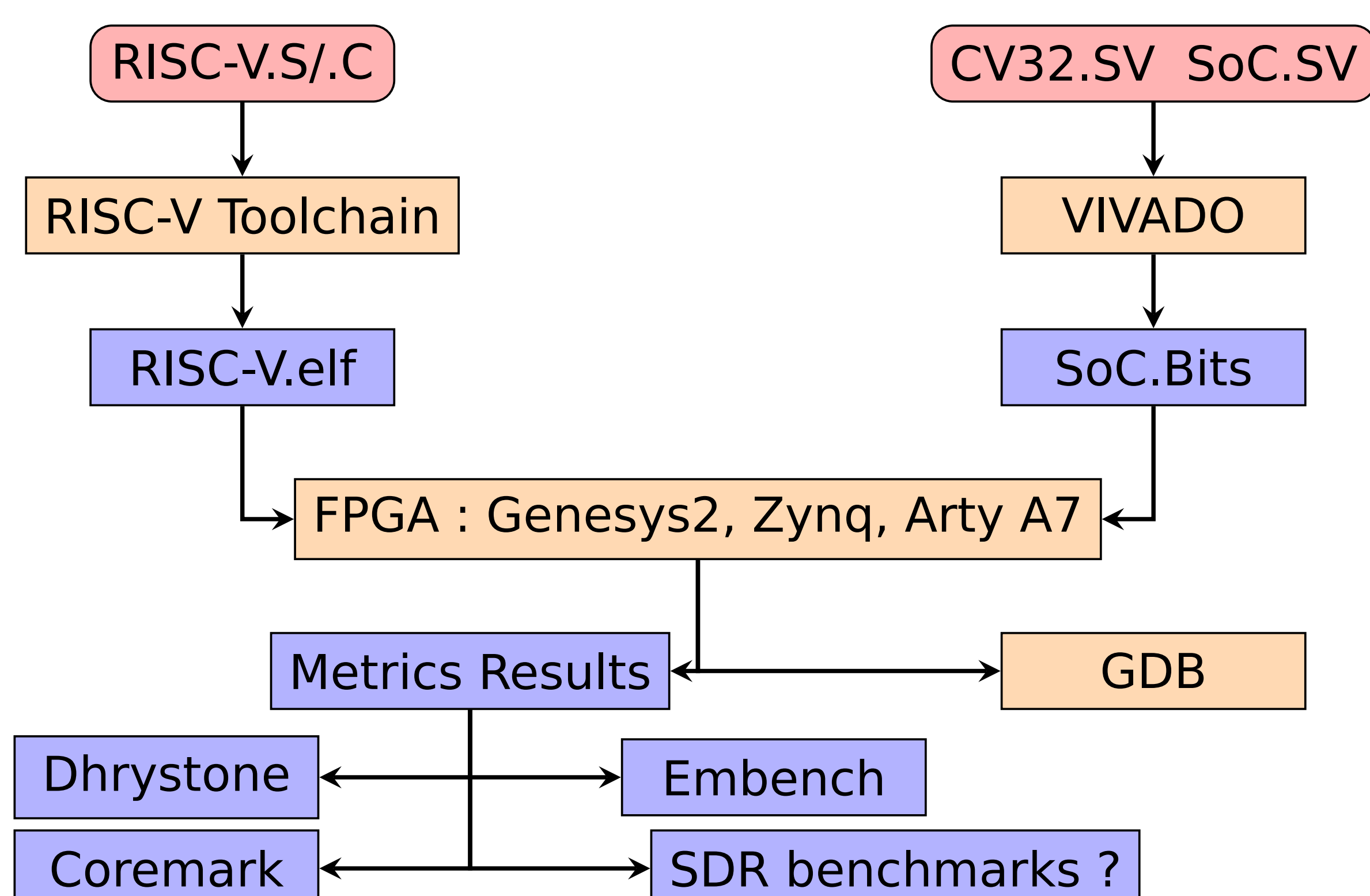
- The emergence of low-cost high-performance platforms and associated software allows attackers to access lower layers of networks [4]
- 33 vulnerabilities in TCP/IP stacks which allows to perform code execution, DoS, and data ex-filtration [5]
- Exploitation of buffer overflow vulnerabilities to perform DoS attacks and remote execution of malware on the target [6]
- Wazabee: Transmitting and receiving 802.15.4 frames, including Zigbee, from a chip supporting only Bluetooth Low Energy (BLE) [7]

Potential threat models

- Jamming Attack ✓
- Logical Attacks: Packet Injection, ... ✓
- Physical Attacks X



Workflow of performance evaluation



Security Mechanisms

- Compilation & run-time levels
- Memory protection and isolation
- Intrusion detection
- Over the air (OTA) programming

Conclusion and perspective work

- CV32E40P RISC-V Processor instruction set extension
- Support DSP performance and Security mechanisms for sub-GHz Protocols
- Reproduction of the authors' work of DSP instructions [3]
- Performance rating (SDR and security benchmarks)

Bibliography

- [1] M. Hessar, A. Najafi, V. Iyer u. a., "TinySDR : Low-Power SDR Platform for Over-the-Air Programmable IoT Testbeds," *Proc. of NSDI*, 2020.
- [2] Y. Chen, S. Lu, H. S. Kim u. a., "A low power software-defined-radio baseband processor for the Internet of Things," *Proceedings - International Symposium on High-Performance Computer Architecture*, Jg. 2016-April, S. 40-51, 2016, ISSN: 15300897. DOI: 10.1109/HPCA.2016.7446052.
- [3] H. Belhadj Amor, C. Bernier and Z. Prikryl, "A RISC-V ISA Extension for Ultra-Low Power IoT Wireless Signal Processing," *IEEE Transactions on Computers*, 2021, ISSN: 15579956. DOI: 10.1109/TC.2021.3063027.
- [4] L. Microsystems, *LimeSDR mini*, <https://limemicro.com/>, [Online; accessed 06-June-2021], 2017.
- [5] F. R. Labs, *AMNESIA:33, How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices*, <https://www.forescout.com/research-labs/amnesia33/>, [Online; accessed 06-June-2021], 2020.
- [6] S. D. Hitefield, M. Fowler and T. C. Clancy, "Exploiting Buffer Overflow Vulnerabilities in Software Defined Radios," *IEEE 2018*, S. 1921-1927, 2018. DOI: 10.1109/Cybermatics_2018.2018.00318.
- [7] R. Cayre, F. Galtier, G. Auriol u. a., "WazaBee: attacking Zigbee networks by diverting Bluetooth Low Energy chips," in *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Taipei (virtual), Taiwan, Juni 2021. Adresse: <https://hal.laas.fr/hal-03193299>.